

ABSTRACT OF THE DISCLOSURE

5 A combinational circuit comprises: a plurality of multipliers, independently performing two or more multiplications for coded digital signals in a Galois extension field $GF(2^m)$ (m is an integer equal to or greater than 2), wherein the multipliers include an input side XOR
10 calculator, an AND calculator, and an output side XOR calculator, and wherein the multipliers share the input side XOR calculator. Further, according to the present invention, these multipliers each include an adder connected between an AND calculator and an output side XOR calculator,
15 wherein the output side XOR calculator is used in common, and wherein the outputs of the AND calculators in the multipliers are added by the adders, and the addition results are calculated by the output side XOR calculator that is used in common.

20